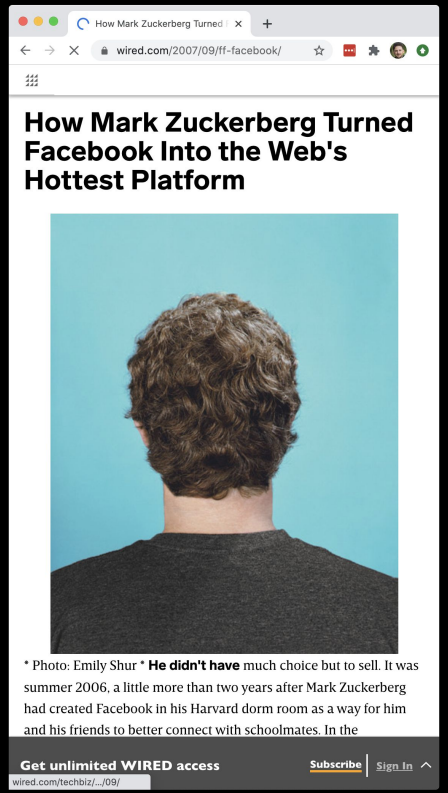
First, a Story

About a DDOS Attack on my FB App in 2007.

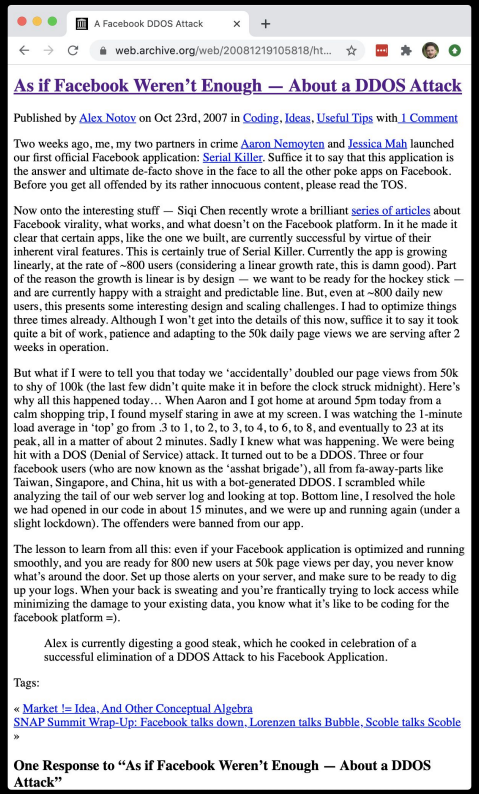
The Year was 2007

I was just coming off an Adobe Labs contract and thought I was super cool.

So I Moved to Cali and Built a FB Game



But the FB Game got DDOSed



A Facebook DDOS Attack

web.archive.org/web/20081219105818/ht...

As if Facebook Weren't Enough — About a DDOS Attack

Published by Alex Notov on Oct 23rd, 2007 in Coding, Ideas, Useful Tips with 1 Comment

Two weeks ago, me, my two partners in crime Aaron Nemoyten and Jessica Mah launched our first official Facebook application: Serial Killer. Suffice it to say that this application is the answer and ultimate de-facto shove in the face to all the other poke apps on Facebook. Before you get all offended by its rather innocuous content, please read the TOS.

Now onto the interesting stuff — Siqi Chen recently wrote a brilliant series of articles about Facebook virality, what works, and what doesn't on the Facebook platform. In it he made it clear that certain apps, like the one we built, are currently successful by virtue of their inherent viral features. This is certainly true of Serial Killer. Currently the app is growing linearly, at the rate of ~800 users (considering a linear growth rate, this is damn good). Part of the reason the growth is linear is by design — we want to be ready for the hockey stick — and are currently happy with a straight and predictable line. But, even at ~800 daily new users, this presents some interesting design and scaling challenges. I had to optimize things three times already. Although I won't get into the details of this now, suffice it to say it took quite a bit of work, patience and adapting to the 50k daily page views we are serving after 2 weeks in operation.

But what if I were to tell you that today we 'accidentally' doubled our page views from 50k to shy of 100k (the last few didn't quite make it in before the clock struck midnight). Here's why all this happened today… When Aaron and I got home at around 5pm today from a calm shopping trip, I found myself staring in awe at my screen. I was watching the 1-minute load average in 'top' go from .3 to 1, to 2, to 3, to 4, to 6, to 8, and eventually to 23 at its peak, all in a matter of about 2 minutes. Sadly I knew what was happening. We were being hit with a DOS (Denial of Service) attack. It turned out to be a DDOS. Three or four facebook users (who are now known as the 'asshat brigade'), all from fa-away-parts like Taiwan, Singapore, and China, hit us with a bot-generated DDOS. I scrambled while analyzing the tail of our web server log and looking at top. Bottom line, I resolved the hole we had opened in our code in about 15 minutes, and we were up and running again (under a slight lockdown). The offenders were banned from our app.

The lesson to learn from all this: even if your Facebook application is optimized and running smoothly, and you are ready for 800 new users at 50k page views per day, you never know what's around the door. Set up those alerts on your server, and make sure to be ready to dig up your logs. When your back is sweating and you're frantically trying to lock access while minimizing the damage to your existing data, you know what it's like to be coding for the facebook platform =).

> Alex is currently digesting a good steak, which he cooked in celebration of a successful elimination of a DDOS Attack to his Facebook Application.

Tags:

« Market != Idea, And Other Conceptual Algebra
SNAP Summit Wrap-Up: Facebook talks down, Lorenzen talks Bubble, Scoble talks Scoble »

One Response to "As if Facebook Weren't Enough — About a DDOS Attack"

We went from 50k page views to 100k page views in 2 minutes.

The Access Log was not Pretty

```
$ tail -f 100
/var/log/apache2/access
.log
```
was overflowing with IP addresses from East Asia.

Users Saw “500” Errors

```
$ tail -f -100
/var/log/apache2/error.
log was overflowing with 500
Internal Server Error.
```

Load Average Spiked to 23!

In `$ top` the load average jumped from 0.3, to 1, to 2, to 3, to 4, to 6, to 8, and eventually to 23 in 2 minutes!

Who am I?

I am Alex Notov.
Lead Enterprise Instructor @ Galvanize.
Humble*d* Student of Security.

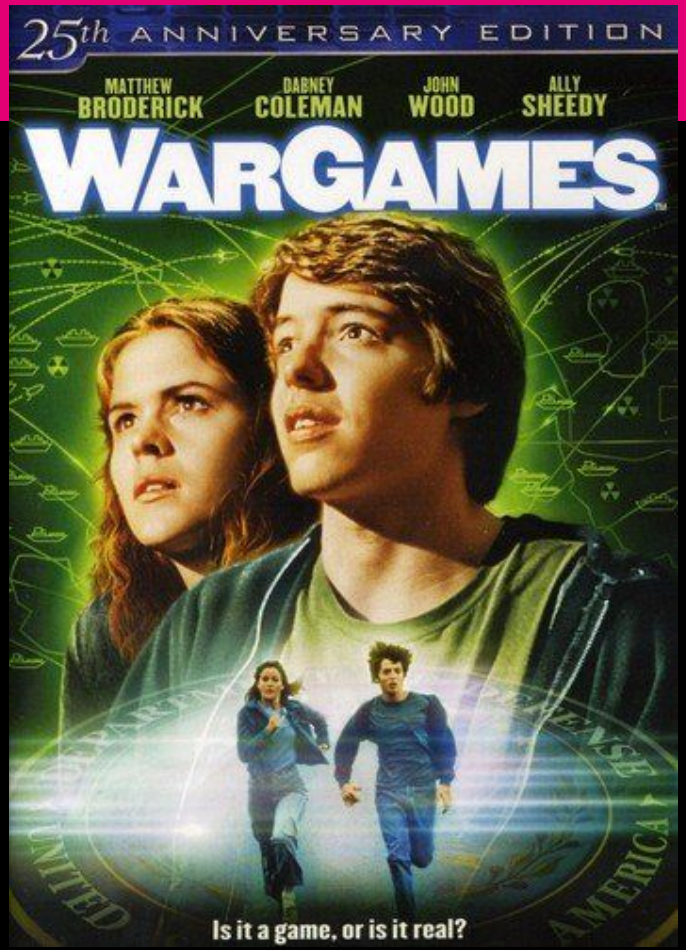
Zero-Trust Security Model

A Philosophical and Practical Discussion

Today's Objectives

Describe vulnerabilities in a simple sample vulnerable application from the perspective of a zero-trust philosophy and its core mantra.

Utilize P&T Security Solutions team's resources to execute on its vision for continuously improving the security posture of code at T-Mobile.



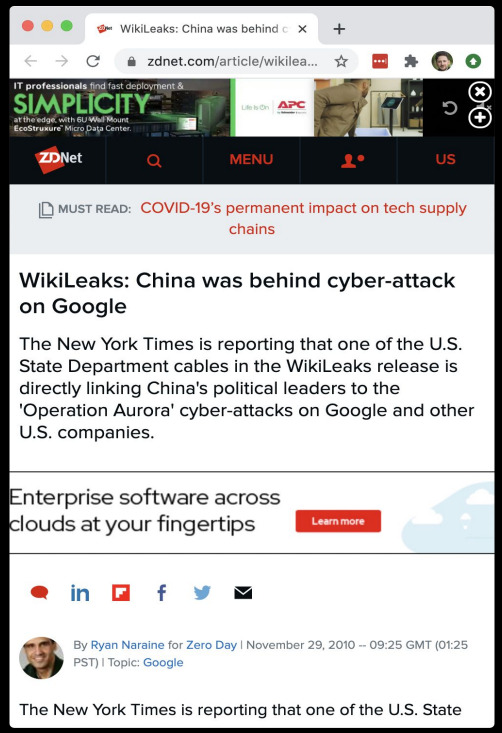
“Shall we play a game?”

Security on the Perimeter

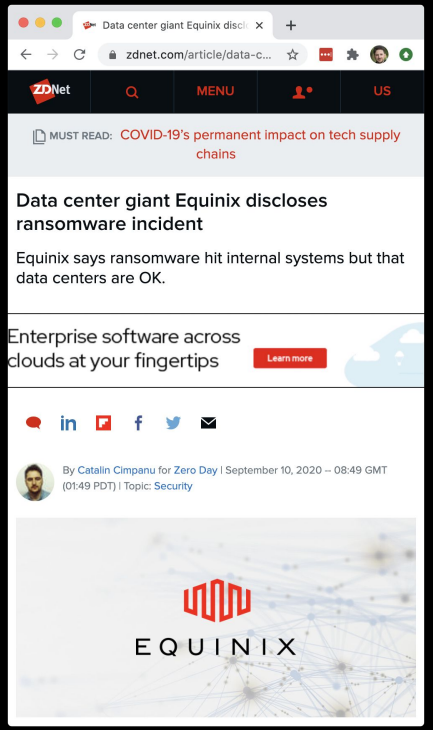
In “War Games,” David got in through a backdoor and could have started WWIII!

What WWIII Looked Like Then

Operation Aurora (2010)



What WWIII Looks Like Today



The Zero-Trust Security Mantra

“Never Trust, Always Verify”

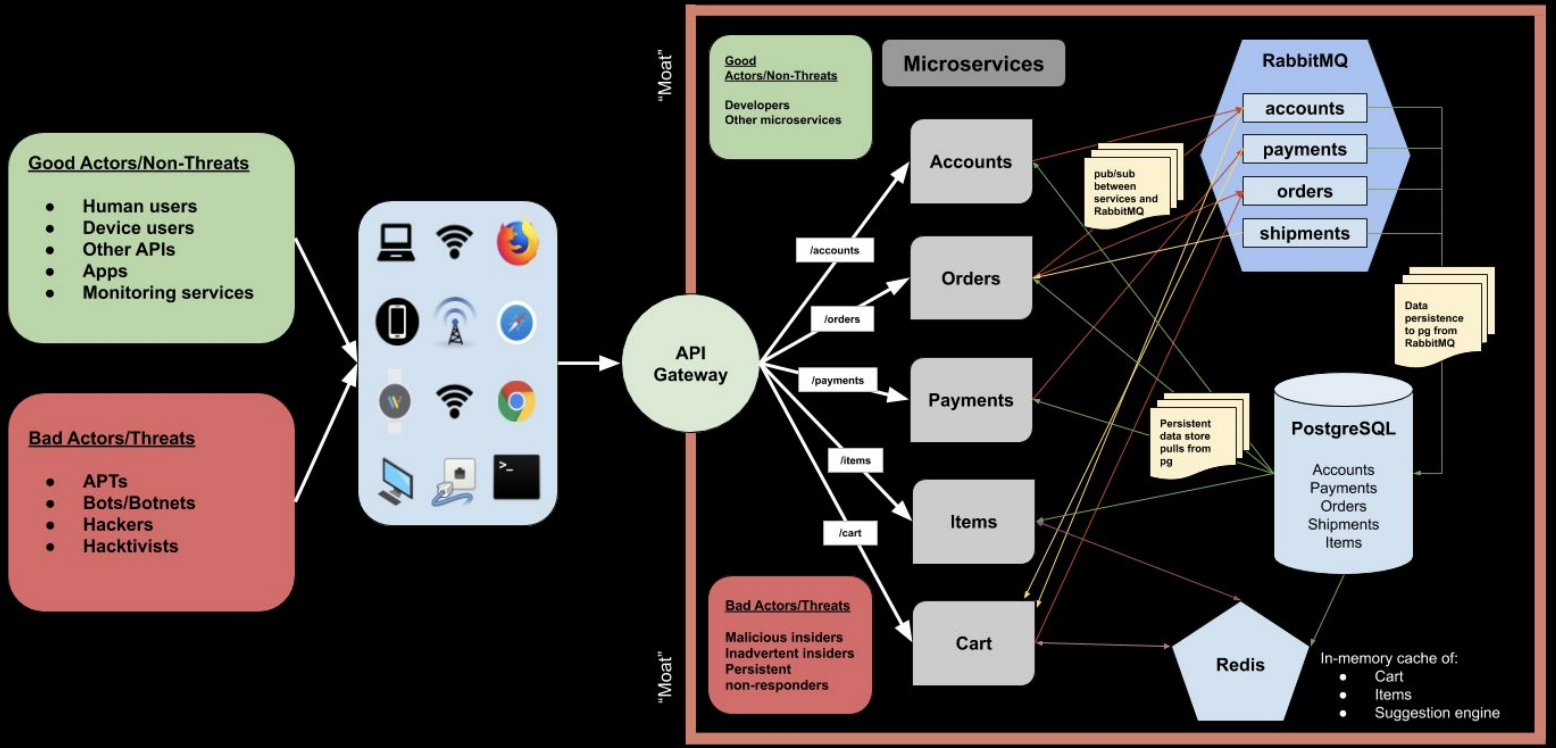
John Kindervag

- Creator of Zero Trust
- Currently at Palo Alto Networks as Field CTO

Castle with a Moat

“Château de la Mothe-Chandeniers”
Les Trois-Moutiers, France

Simple Sample Vulnerable Shopping App



What Can You Do Once Inside the Castle?

Once behind the “moat,” what do you have access to?

What Can You Do Once Inside the Castle?

Why do you have access to it?

What Can You Do Once Inside the Castle?

Should you?

The Zero-Trust Security Mantra

“Never Trust, Always Verify”

What Are Some Possible Solutions?

Was the sigil verified at the gate?

What Are Some Possible Solutions?

User inventory and identity management

What Are Some Possible Solutions?

Was the carriage suspicious?

What Are Some Possible Solutions?

Device inventory and management

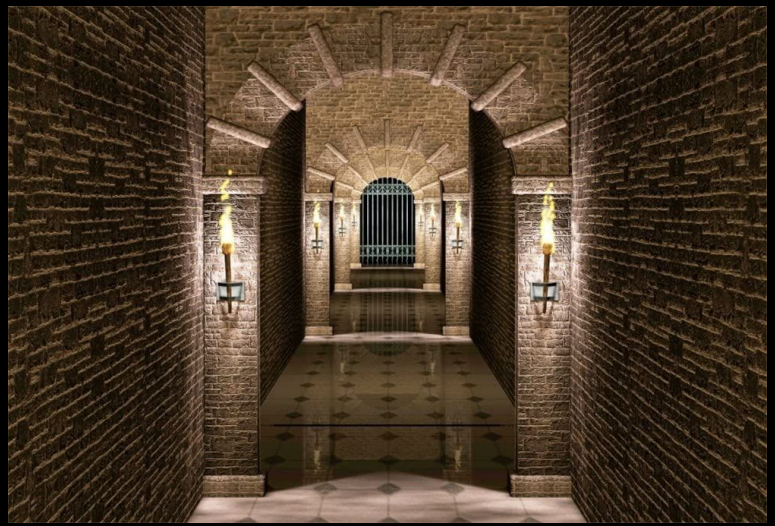
What Are Some Possible Solutions?

Did you come via an expected secured route?

What Are Some Possible Solutions?

Encryption in transit

What Are Some Possible Solutions?



Once inside, what rooms can you access?

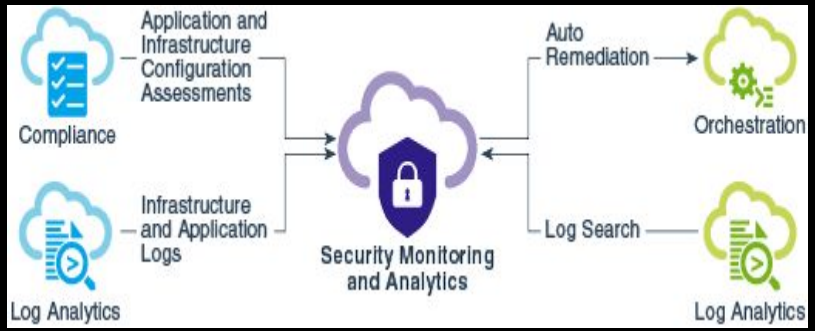
What Are Some Possible Solutions?

Security policy and enforcement

What Are Some Possible Solutions?

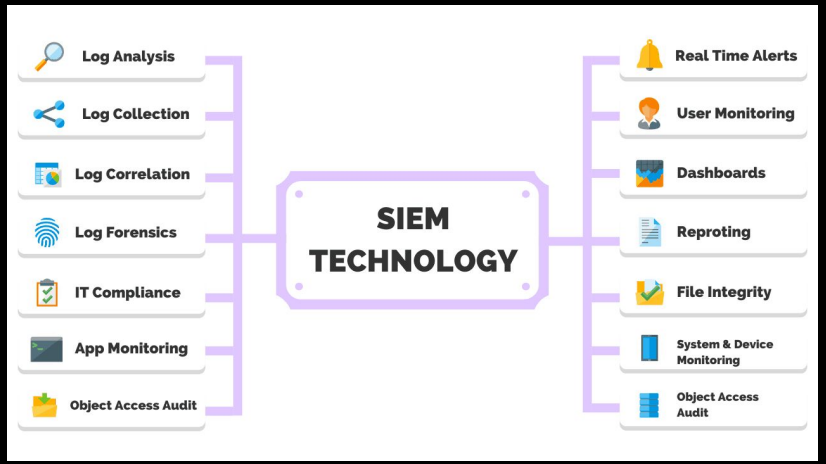
Is someone watching your movements through the castle?

What Are Some Possible Solutions?



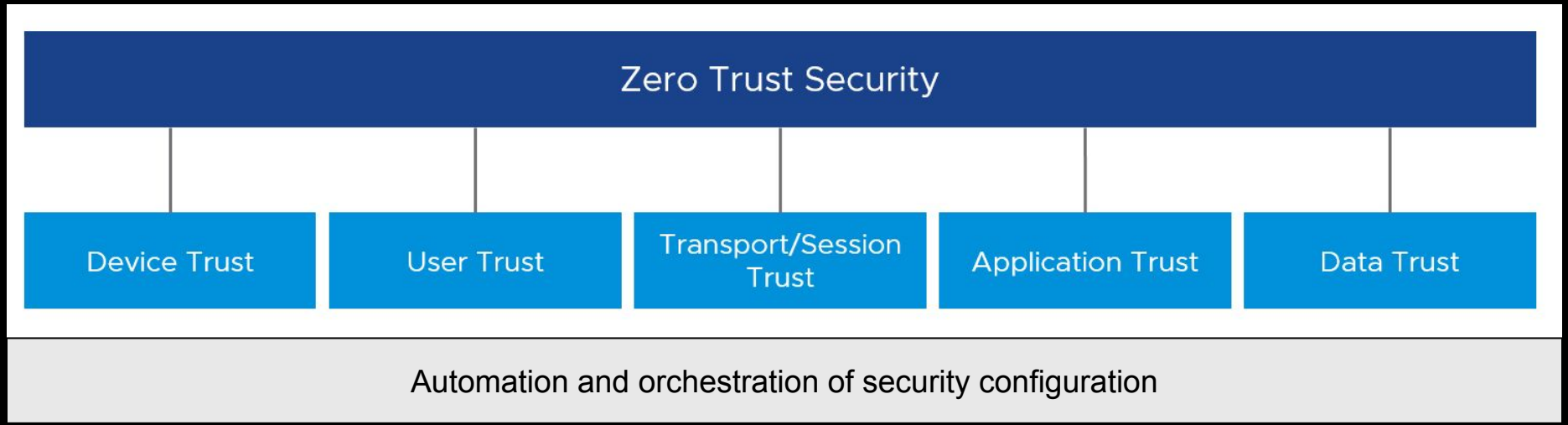
Security monitoring and analytics

What Are Some Possible Solutions?



Automated SIEM as Code & SOAR

The Pillars of Zero Trust



An Example from T-Mobile Land

When will I be asked for MFA?

You will be asked for MFA per policy configurations based on several factors such as location, device, application, etc.. For example, you may be prompted for MFA if you are accessing an application from outside the corporate network versus inside the network. You will be provided instructions and prompted in the event an MFA is required.